F I L E D
United States Court of Appeals
Tenth Circuit

October 26, 2005

Clerk of Court

PUBLISH

UNITED STATES COURT OF APPEALS

TENTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. BRENT RAY BROOKS, Defendant-Appellant.	No. 04-4255

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH, CENTRAL DIVISION
(D.C. NO. 03-CR-751-PGC)

Steven B. Killpack, Federal Public Defender (Scott Keith Wilson, Assistant Federal Public Defender, with him on the briefs), Office of the Federal Public Defender, Salt Lake City, Utah for Defendant-Appellant.

Paul G. Amann, Special Assistant United States Attorney (Paul M. Warner, United States Attorney, with him on the brief), Office of the United States Attorney, Salt Lake City, Utah for Plaintiff-Appellee.

Before **McCONNELL**, **McKAY**, and **TYMKOVICH**, Circuit Judges.

TYMKOVICH, Circuit Judge.

Brent Ray Brooks was indicted for receipt of child pornography in violation of 18 U.S.C. § 2252A(a)(2)(A), possession of child pornography in violation of 18 U.S.C. § 2252A(5)(B), and distribution of child pornography in violation of 18 U.S.C. § 2242A(a)(1). He entered a conditional plea of guilty to the charge of possession of child pornography and preserved his right to appeal the district court's denial of his motion to suppress evidence found on his computer.

In his appeal, Brooks argues (1) that officers exceeded the scope of his consent when they searched his computer by means other than those explained to him in the course of obtaining consent; and (2) that the warrant for the computer search was not adequately specific. We take jurisdiction pursuant to 28 U.S.C. § 1291 and affirm.

I. BACKGROUND

On August 26, 2003, Utah County law enforcement officers responded to a report of an unattended child at Brooks's house. When they arrived, they detected the odor of marijuana inside the residence. Thereafter, they obtained a search warrant (the "first warrant") authorizing a search for items associated with marijuana use. During their search the following day they found a substantial amount of what appeared to be child pornography in one of Brooks's garbage cans. After this discovery, officers obtained another warrant on August 27, 2003 (the "second warrant") authorizing a search of Brooks's home, including any

computer equipment, for child pornography. They also contacted Special Agent Brian Snyder, an FBI agent with experience in child pornography and child exploitation investigations, to assist with their search. Law enforcement executed the warrant on the same day.

Since the pornographic images found in Brooks's garbage appeared to have been printed from a computer printer, officers "assume[d] that there [was] possibly more child pornography on the [home] computer[.]" ROA, Vol. IV at 11. Accordingly, upon his arrival Agent Snyder requested permission from Brooks to search Brooks's computer. Snyder explained to Brooks that the search would involve inserting a "pre-search" disk into his computer. Although the record is unclear as to precisely how the disk functioned, it apparently contained a program that searched for image files and displayed the images in a thumbnail format so a viewer could easily ascertain whether the images included child pornography. Agent Snyder further explained to Brooks that the disk would not search for text files, but would search for and display only image files.

Brooks told Snyder that he had "nothing to hide" and agreed to sign a search consent form. The form stated that Brooks (1) had been asked by the FBI to authorize a "complete search" including a "pre-search for child pornography" of his computer tower; (2) had been advised of his right to refuse consent; (3) gave his consent voluntarily; and (4) authorized agents to take any items they determined were related to their investigation. ROA, Vol. IV, Exhibit F.

After obtaining Brooks's consent to search the computer, Snyder went to the computer and inserted the pre-search disk. The computer was already turned on. For reasons the record does not make clear, the disk did not function on the computer. Thus, Agent Snyder decided to attempt a manual search for image files through the computer's "file search" function. He was unable to complete the manual review, however, because Brooks's computer prompted him to enter a password. Snyder therefore returned to Brooks and asked him for the password to the computer, which Brooks told him was the same as the log-on password. After this conversation Agent Snyder went back to Brooks's computer and completed the process of a manual image file search.

Snyder located several images of adolescent male boys engaged in sexual activity. He did not view or open any text files. After Snyder viewed the images, officers shut down the computer and seized it. They subsequently obtained a third warrant authorizing a search of three computers, twelve compact disks, and seven diskettes located at Brooks's residence. This forensic search was carried out at a police laboratory.

Brooks later moved to suppress the pornographic images found during (1) Snyder's manual search, and (2) the laboratory's forensic search. The district court denied the motion. Brooks then entered a conditional guilty plea on May 3, 2004, and on October 14, 2004, the United States District Court for the District of

Utah sentenced him to 88 months in prison and 156 months of supervised release. Pursuant to the conditional plea, Brooks filed this appeal.

II. DISCUSSION

Brooks argues on appeal (A) that officers exceeded the scope of his consent when they searched his computer by means other than those explained to him in the course of obtaining written consent; and (B) that the warrant for the computer search was not adequately specific.

A. Scope of the Search

We uphold the factual findings of a district court made in connection with a motion to suppress unless those findings are clearly erroneous, *United States v. Williams*, 271 F.3d 1262, 1266 (10th Cir. 2001) (citing *United States v. Hunnicutt*, 135 F.3d 1345, 1348 (10th Cir. 1998)), and we must view the evidence in the light most favorable to the determination of the district court. *Id*. (citing *United States v. West*, 219 F.3d 1171, 1176 (10th Cir. 2000)). We review the district court's legal findings de novo. *United States v. Minjares-Alvarez*, 264 F.3d 980, 983-84 (10th Cir. 2001).

It is well settled that voluntary consent can obviate the warrant requirement of the Fourth Amendment. *See Schneckloth v. Bustamonte*, 412 U.S. 218, 227 (1973). However, "[t]he scope of a search . . . is limited by the breadth of the consent given." *United States v. Elliott*, 107 F.3d at 814-15 (10th Cir. 1997) (internal citations omitted). We apply an "objective reasonableness" standard to

the scope of consent, asking what "would the typical reasonable person have understood by the exchange[.]" *Id*. We examine the totality of the circumstances when determining whether a search was within the scope of the consent. *United States v. Gutierrez-Hermosillo*, 142 F.3d 1225, 1231 (10th Cir. 1998).

As a preliminary matter, the record shows that Brooks never explicitly argued to the district court that the officers' search exceeded his consent. His only argument to the district court was that his consent to the home seach was not knowingly and voluntarily given. Accordingly, since Brooks failed to raise the issue below, we review for plain error. *See United States v. Walser*, 275 F.3d 981, 985 (10th Cir. 2001). We find no error here. The record is clear that the officers did not expand their search of Brooks's computer nor overstep the bounds of Brooks's consent. As previously discussed, at the point Agent Snyder obtained Brooks's permission to search the computer, Snyder told Brooks the search would be conducted with a computer disk that would automatically search for image files. Brooks argues that his consent was therefore limited to the specific software-driven pre-search Snyder initially described, and the images obtained during Snyder's subsequent manual search should have been suppressed. We disagree that the search exceeded an objectively reasonable interpretation of Brooks's consent for several reasons.

First, the scope of Snyder's search did not, in fact, exceed the permission Brooks granted in his written consent. In the consent form, Brooks agreed to the

following: a "complete search" of the "CPU tower . . . belonging to Brent Brooks to conduct a pre-search for child pornography." ROA, Vol. I, Exhibit F. While the officers intended to use a computer tool to assist the search, the actual manual search did nothing more than what Brooks had authorized. The terminology in the consent form regarding a "pre-search" is somewhat confusing. What is not confusing is the fact, as determined by the district court, that Brooks understood his computer was to be searched for pornographic images and voluntarily consented to such a search.

Second, in the face of this written authorization, Brooks argues that his conversations with Agent Snyder implicitly limited the scope of the search. On this record, however, Snyder's actual search does not appear to exceed the scope of the disk search he orally described to Brooks. As counsel explained at oral argument, the pre-search disk searches the computer hard drive for image files, then displays them for review. An officer must then review those images for pornographic material. What Agent Snyder did manually was the functional equivalent of employing the pre-search disk—he ran a search for image files, them viewed them to determine whether they contained child pornography. We see no discernable difference between the search to which Brooks says he consented and the search that actually occurred, and Brooks has not provided us a reason to believe otherwise.

Brooks counters these facts by arguing that our precedent requires a narrow construction of the scope of consent. *See, e.g., United States v. Elliott*, 107 F.3d 810 (10th Cir. 1997). In *Elliott*, the officer requested permission to "look through the trunk [of the defendant's car] and see what you got in there." The officer further stated that he did not "want to look through each item" and merely wanted to ascertain how the bags were "packed" or "packaged" in the trunk. *Id.* at 815. After the defendant consented to the search as described by the officer, the officer proceeded to open a zipped bag in the trunk. Inside the bag he discovered marijuana. This court held that because the officer "expressly and narrowly limited the scope of his request, it is apparent that [he] exceeded the scope of [the defendant's consent] and thereby violated her Fourth Amendment rights by unzipping and looking inside one of the bags in the trunk." *Id.* at 815-16.

Unlike the plaintiff in *Elliott*, who could show the actual search differed substantially from the proffered search, Brooks is unable to supply a reason why Snyder's manual search process exceeded the permission granted. Snyder stayed well within the boundaries of the search that had been authorized, searching only for image files. His manual search was no more invasive than the automated one he described to Brooks; Snyder viewed no text files, opened no additional electronic folders, and completed no searches that the disk would not have completed. Once Snyder viewed several images and confirmed the presence of pornography, he turned off the computer. After examining the record, we cannot

conclude Snyder's search differed substantially from the search that would have transpired had he used the pre-search disk; Snyder simply entered certain commands manually instead of allowing this work to be done by a pre-programmed disk. Accordingly, these circumstances can hardly be compared to the situation in *Elliott*, where, after explicitly stating they would not do so, officers opened zipped bags and searched them.

Our conclusion is bolstered by the circumstances surrounding this search. In this case, officers scrupulously sought warrants every step of the way and were careful not to overstep the boundaries of Brooks's initial consent to conduct the pre-search. Even before Snyder began the pre-search, officers were already in the process of seeking a warrant to seize Brooks's computers. More importantly, Snyder viewed only a few images on Brooks's computer before turning off the computer, seeking the advice of counsel, and then obtaining the forensic search warrant from a neutral magistrate for the completion of the search.

Accordingly, we conclude the search was within the scope of Brooks's consent, and the district court did not commit plain error in denying Brooks's motion to suppress on this ground.

B. The Computer Search Warrant

The Fourth Amendment requires that a search warrant "describe the things to be seized with sufficient particularity to prevent a general exploratory rummaging in a person's belongings." *United States v. Campos*, 221 F.3d 1143,

1147 (10th Cir. 2000). In considering whether the warrants at issue describe the items to be seized with sufficient particularity, we accept the district court's factual findings unless clearly erroneous. However, the district court's ultimate determination of sufficient particularity is reviewed de novo. *United States v. Leary,* 846 F.2d 592 (10th Cir. 1988).

"The manifest purpose of [the] particularity requirement was to prevent general searches. By limiting the authorization to search the specific areas . . . the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *United States v. Riccardi*, 405 F.3d 852, 863 (10th Cir. 2005) (citing *Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *Voss v. Bergsgaard*, 774 F.2d 402, 404 (10th Cir. 1985); *Campos*, 221 F.3d at 1147)).

Brooks argues that the third warrant, which authorized a laboratory search of his computer equipment, was not sufficiently particular for two reasons. First, he argues it failed to describe a specific search methodology for use on the computer. Second, he claims it allowed investigators to search for and view text files that may not have included pornographic images.

Search Methodology. At the outset, we disagree with Brooks that the government was required to describe its specific search methodology. This court has never required warrants to contain a particularized computer search strategy.

We have simply held that officers must describe with particularity the *objects of their search*. Recognizing the difficulties inherent in computer searches, in some circumstances, we have suggested that "law enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant." *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999). As we explained in *Carey*, "[w]here officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate . . . [t]he magistrate should then require officers to specify in a warrant which type of files are sought." *Id.* However, we have not required a specific prior authorization along the lines suggested in *Carey* in every computer search, *see, e.g., Campos*, 221 F.3d at 1147, nor has Brooks suggested how the search in this case would have been different with a scripted search protocol.

The question of whether the nature of computer forensic searches lends itself to predetermined search protocols is a difficult one. Given the numerous ways information is stored on a computer, openly and surreptiously, a search can be as much an art as a science. *See Carey*, 172 F.3d 1268 (10th Cir. 1999).[1] But as we noted in *Carey* and *Campos*, courts will look to (1) the object of the search,

[1] An interesting article on the challenges in this area can be found in Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. (forthcoming 2006), *available at* http://ssrn.com/abstract=697541.

(2) the types of files that may reasonably contain those objects, and (3) whether officers actually expand the scope of the search upon locating evidence of a different crime. Both *Carey* and *Campos* involved warrants less detailed than the one here. In *Carey*, while searching for drug crime evidence, officers came across evidence of child pornography, and without authorization they expanded their search of a computer for additional pornographic images. In *Campos*, the warrant broadly allowed for the seizure of a computer without any specific reason to believe it actually contained child pornography. The question in those cases was whether additional authorization for an expanded search was necessary. They do not, however, stand for the proposition that a warrant is per se overbroad if it does not describe a specific search methodology.

We thus find in the circumstances here that the warrant need not have included a search protocol to satisfy the particularity requirement of the Fourth Amendment.

Scope of Warrant. We now turn to Brooks's second overbreadth argument. The warrant authorized officers to search two computers and a number of disks "for evidence of child pornography," including

> "photographs, pictures, computer generated pictures or images, depicting partially nude or nude images of prepubescent males and or females engaged in sex acts,". . . as well as "correspondence, including printed or handwritten letters, electronic text files, emails and instant messages[.]"

ROA, Vol. I at 62; Aplt. Br. Attach. B. While the warrant does not explicitly instruct officers to look solely for those text files containing child pornography, in context—and certainly in the view of the officers conducting the search—the restrictions placed upon searches for image files also apply to the other types of files. In other words, although the language of the warrant may, on first glance, authorize a broad, unchanneled search through Brooks's document files, as a whole, its language more naturally instructs officers to search those files only for evidence *related to child pornography*. In this light, the warrant should be—and was—read by officers to implicitly place the same restriction (*i.e.*, to locate child pornography) on the scope of the entire search.

Brooks, however, argues that our cases have required "a more particularized inquiry" than the warrant here describes. *See Riccardi*, 405 F.3d at 862 (citing *Campos*, 221 F.3d at 1147). We disagree that this requirement has not been met. In *Riccardi*, the warrant at issue in a child pornography investigation authorized the "seizure" of the defendant's computer and "all electronic and magnetic media stored therein, together with all storage devises [sic], internal or external to the computer or computer system." *Riccardi,* 405 F.3d at 862. On review, we found that "[b]y its terms, the warrant thus permitted the officers to search for anything—from child pornography to tax returns to private correspondence," making it "precisely the kind of 'wide-ranging exploratory

search that the Framers intended to prohibit.'" *Id.* at 863 (citing *Maryland v. Garrison*, 480 U.S. 79, 84 (1987)).

Here, in contrast, we are faced with a warrant that authorized officers to search through computer files for particular items specifically related to child pornography. The warrant language is properly read to place the very same subject matter restriction on the authorization to search Brooks's text files as it clearly placed on searches of his image files. Moreover, Brooks has made no showing that officers improperly viewed text files, or expanded the scope of the search for materials other than child pornography. While the warrant could have been more artfully written, we are satisfied on these facts that it falls within the particularity requirement of the Fourth Amendment.

III. CONCLUSION

Accordingly, we AFFIRM the district court's judgment.